

6

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Shunpei YAMAZAKI et al. Art Unit : Unknown
Serial No. : Not assigned yet Examiner : Unknown
Filed : April 26 2001
Title : A SYSTEM FOR IDENTIFYING AN INDIVIDUAL, A METHOD FOR
IDENTIFYING AN INDIVIDUAL OR A BUSINESS METHOD



Commissioner for Patents
Washington, D.C. 20231

TRANSMITTAL OF PRIORITY DOCUMENT UNDER 35 USC §119

Applicant hereby confirms his claim of priority under 35 USC §119 from the following application: Japan Application No. 2000-126513 filed April 26, 2000. A certified copy of each application from which priority is claimed is submitted herewith.

Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: April 26, 2001

William D. Hare
William D. Hare
Reg. No. 44,739

Fish & Richardson P.C.
601 Thirteenth Street, NW
Washington, DC 20005
Telephone: (202) 783-5070
Facsimile: (202) 783-2331

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

JC903 U.S. PTO
09/842219
04/26/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

2000年 4月26日

出 願 番 号
Application Number:

特願2000-126513

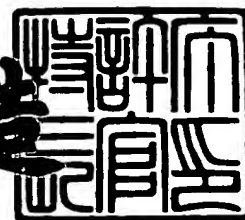
出 願 人
Applicant(s):

株式会社半導体エネルギー研究所

2001年 3月 2日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2001-3012556

【書類名】 特許願

【整理番号】 P004876

【提出日】 平成12年 4月26日

【あて先】 特許庁長官 殿

【発明者】

 【住所又は居所】 神奈川県厚木市長谷 3 9 8 番地 株式会社半導体エネルギー研究所内

 【氏名】 山崎 舜平

【発明者】

 【住所又は居所】 神奈川県厚木市長谷 3 9 8 番地 株式会社半導体エネルギー研究所内

 【氏名】 小山 潤

【特許出願人】

 【識別番号】 000153878

 【氏名又は名称】 株式会社半導体エネルギー研究所

 【代表者】 山崎 舜平

【手数料の表示】

 【予納台帳番号】 002543

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 本人認証システム

【特許請求の範囲】

【請求項 1】

顧客を識別する本人認証システムであって、
前記顧客の生体情報を記憶する手段と、
前記顧客の生体情報を読み取る手段と、
前記読み取った生体情報を前記記憶した生体情報と照合する手段と、
前記照合が合致した場合、サーバーに合致したことを情報として送る手段と、
を有することを特長とする本人認証システム。

【請求項 2】

顧客を識別する本人認証システムであって、
前記顧客の複数の生体情報を記憶する手段と、
前記顧客の生体情報を読み取る手段と、
前記読み取った生体情報を前記記憶した複数の生体情報と照合する手段と、
前記読み取った生体情報が、前記記憶した複数の生体情報のうち少なくとも 1
つと合致した場合、サーバーに合致したことを情報として送る手段と、
を有することを特長とする本人認証システム。

【請求項 3】

顧客を識別する本人認証システムであって、
前記顧客の複数の生体情報を記憶する手段と、
前記顧客の複数の生体情報を読み取る手段と、
前記読み取った複数の生体情報を前記記憶した複数の生体情報と照合する手段
と、
前記読み取った複数の生体情報のそれぞれが、前記記憶した複数の生体情報の
うち少なくとも 1 つと合致した場合、サーバーに合致したことを情報として送る
手段と、
を有することを特長とする本人認証システム。

【請求項 4】

顧客を識別する本人認証システムであって、
前記顧客の生体情報を記憶する手段と、
前記顧客の生体情報を読み取る手段と、
前記読み取った生体情報を前記記憶した生体情報と照合する手段と、
前記照合が合致した場合、サーバーに合致したことを情報として、インターネットを介して送る手段と、
を有することを特長とする本人認証システム。

【請求項 5】

顧客を識別する本人認証システムであって、
前記顧客の複数の生体情報を記憶する手段と、
前記顧客の生体情報を読み取る手段と、
前記読み取った生体情報を前記記憶した複数の生体情報と照合する手段と、
前記照合の結果、前記読み取った生体情報が、前記記憶した複数の生体情報のうち少なくとも 1 つと合致した場合、サーバーに前記照合が合致したことを情報として、インターネットを介して送る手段と、
を有することを特長とする本人認証システム。

【請求項 6】

顧客を識別する本人認証システムであって、
前記顧客の複数の生体情報を記憶する手段と、
前記顧客の複数の生体情報を読み取る手段と、
前記読み取った複数の生体情報を前記記憶した複数の生体情報と照合する手段と、

前記照合の結果、前記読み取った複数の生体情報のそれぞれが、前記記憶した複数の生体情報のうち少なくとも 1 つと合致した場合、サーバーに前記照合が合致したことを情報として、インターネットを介して送る手段と、
を有することを特長とする本人認証システム。

【請求項 7】

顧客を識別する本人認証システムであって、
前記顧客の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、
前記読み取った生体情報を前記記憶した生体情報と照合する手段と、
前記照合が合致した場合、サーバーに合致したことを情報として送る手段と、
前記サーバーが前記顧客の取引先に前記照合が合致したことを情報として送る手段と、
を有し、

前記取引先が、前記照合が合致したことを情報として受け取った後に、前記顧客と前記取引先との間で取引が開始されることを特長とする本人認証システム。

【請求項 8】

顧客を識別する本人認証システムであって、
前記顧客の複数の生体情報を記憶する手段と、
前記顧客の生体情報を読み取る手段と、
前記読み取った生体情報を前記記憶した複数の生体情報と照合する手段と、
前記照合の結果、前記読み取った生体情報が前記記憶した複数の生体情報のうち少なくとも 1 つと合致した場合、サーバーに前記照合が合致したことを情報として送る手段と、
前記サーバーが前記顧客の取引先に前記照合が合致したことを情報として送る手段と、
を有し、

前記取引先が、前記照合が合致したことを情報として受け取った後に、前記顧客と前記取引先との間で取引が開始されることを特長とする本人認証システム。

【請求項 9】

顧客を識別する本人認証システムであって、
前記顧客の複数の生体情報を記憶する手段と、
前記顧客の複数の生体情報を読み取る手段と、
前記読み取った複数の生体情報を前記記憶した複数の生体情報と照合する手段と、

前記照合の結果、前記読み取った複数の生体情報のそれぞれが、前記記憶した複数の生体情報のうち少なくとも 1 つと合致した場合、サーバーに前記照合が合

致したことを情報として送る手段と、

前記サーバーが前記顧客の取引先に前記照合が合致したことを情報として送る手段と、

を有し、

前記取引先が、前記照合が合致したことを情報として受け取った後に、前記顧客と前記取引先との間で取引が開始されることを特長とする本人認証システム。

【請求項 1 0】

顧客を識別する本人認証システムであって、

前記顧客の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した生体情報と照合する手段と、

前記照合が合致した場合、サーバーに合致したことを情報として送る手段と、
を有し、

前記サーバーに前記照合が合致したことを情報として送った後に、暗証番号を情報として前記サーバーに送り、前記サーバーにおいて記憶されている番号と前記暗証番号が合致した場合、前記記憶された生体情報を書き換えられることを特長とする本人認証システム。

【請求項 1 1】

顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した複数の生体情報と照合する手段と、

前記読み取った生体情報が、前記記憶した複数の生体情報のうち少なくとも 1 つと合致した場合、サーバーに合致したことを情報として送る手段と、
を有し、

前記サーバーに前記照合が合致したことを情報として送った後に、暗証番号を情報として前記サーバーに送り、前記サーバーにおいて記憶されている番号と前記暗証番号が合致した場合、前記記憶された複数の生体情報を書き換えられることを特長とする本人認証システム。

【請求項 1 2】

顧客を識別する本人認証システムであって、
前記顧客の複数の生体情報を記憶する手段と、
前記顧客の複数の生体情報を読み取る手段と、
前記読み取った複数の生体情報を前記記憶した複数の生体情報と照合する手段と、

前記読み取った複数の生体情報のそれぞれが、前記記憶した複数の生体情報のうち少なくとも1つと合致した場合、サーバーに合致したことを情報として送る手段と、
を有し、

前記サーバーに前記照合が合致したことを情報として送った後に、暗証番号を情報として前記サーバーに送り、前記サーバーにおいて記憶されている番号と前記暗証番号が合致した場合、前記記憶された複数の生体情報を書き換えられることを特長とする本人認証システム。

【請求項 1 3】

請求項 7 乃至請求項 9 のいずれか 1 項において、前記顧客と前記取引先との間で行われる取引が前記サーバーに設定された条件を満たす場合のみ、前記顧客の識別を要求することを特長とする本人認証システム。

【請求項 1 4】

請求項 1、請求項 4、請求項 7、請求項 1 0 または請求項 1 3 のいずれか 1 項に記載の前記生体情報とは、指紋、掌紋または声紋であることを特長とする本人認証システム。

【請求項 1 5】

請求項 2、請求項 3、請求項 5、請求項 6、請求項 8、請求項 9、請求項 1 1、請求項 1 2 または請求項 1 3 のいずれか 1 項に記載の前記複数の生体情報とは、指紋、掌紋または声紋であることを特長とする本人認証システム。

【請求項 1 6】

請求項 1 4 または請求項 1 5 において、前記掌紋は手ひらの全体の掌紋、もしくは前記手のひらの一部の掌紋であることを特徴とした本人認証システム。

【請求項 1 7】

請求項 1 乃至請求項 1 6 のいずれか 1 項において、前記記憶する手段とは、フラッシュメモリを含むことを特長とする本人認証システム。

【請求項 1 8】

請求項 1 乃至請求項 1 6 のいずれか 1 項において、前記読み取る手段とは、フォトダイオードまたは CCD を含むことを特長とする本人認証システム。

【請求項 1 9】

請求項 1 乃至請求項 1 8 のいずれか 1 項において、
携帯情報端末を用いることを特長とする本人認証システム。

【請求項 2 0】

請求項 1 乃至請求項 1 8 のいずれか 1 項において、
携帯電話を用いることを特長とする本人認証システム。

【請求項 2 1】

請求項 1 乃至請求項 1 8 のいずれか 1 項において、
パーソナルコンピュータを用いることを特長とする本人認証システム。

【0 0 0 0】

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は本人認証システムに関し、特に、生体情報を用いて本人認証を行うことを特徴とした本人認証システムである。

【0 0 0 2】

【従来の技術】

近年、携帯電話、パソコン、携帯情報端末などの通信装置を使用してインターネットに接続する通信技術が急速に発展しつつある。企業、家庭でのインターネット等への接続は、据え置き型のパソコンに電話回線を接続することで行われている。特に近年では、インターネットが簡単に出来る i モードなどの携帯電話が普及し、さまざまな情報交換が簡便に行われるようになった。

【0 0 0 3】

通信装置を用いて、インターネット上で金銭授受などの取引を行う場合、本人であることの確認（本人認証作業）が必要である。本人認証作業は、あらかじめ相手先に登録されている暗証番号を、使用者が通信装置により相手先に送信し、相手先で該暗証番号を照合することで行われている。

【 0 0 0 4 】

図 1 1 に従来の本人認証のフローを示す。使用者はまずインターネットに接続し、取引の相手先の指定した条件下で、認証のための数値を通信装置を用いて相手先に送信する。認証のための数値のデータを受信した相手先は、自分のところにあらかじめ登録された暗証番号と、使用者から送られてきた数値との照合を行い、合致するかどうかを確認する。ここで合致が見られれば、使用者は本人と確認され、要望する対応を得ることができる。

【 0 0 0 5 】

【発明が解決しようとする課題】

上記したような従来の通信装置を用いた認証システムでは以下の問題があった。

- 1、暗証番号が本人以外の人に漏洩した場合、使用者（顧客）以外に悪用される可能性があり、本人であることの確認が難しい。
- 2、本人認証作業の際、使用者から相手先へ暗証番号のデータを送信したり、相手先（サーバー）から使用者へ認証の是非をデータとして送信したりするため、通信するのに必要なコストが上昇する。そして使用者と相手先の間においてデータをやりとりする回数が多いため、何らかのエラーにより通信が断絶すると本人認証作業を最初から再び行う必要が生じ、作業が繁雑である。
- 3、使用者が暗証番号を忘れることで、相手先に再び暗証番号を登録する必要があるが生じる。
- 4、暗証番号を通信機器に入力する際、操作キーの入力に手間がかかる。

【 0 0 0 6 】

本発明は、上記問題を解決することを課題とする。

【 0 0 0 7 】

【課題を解決するための手段】

本発明では本人認証作業を通信装置のみを用いて行い、本人かどうかの確認は、通信装置において使用者の生体情報を照合することで行う。本明細書において生体情報とは、人間が生まれつき持っている身体的な特徴で、なおかつ人間の個体識別が可能な情報を意味し、指紋、掌紋、声紋等が挙げられる。通信装置に使用者の生体情報を入力することで本人認証作業を行い、認証された場合にのみ、相手先に認証されたことを通知する。

【 0 0 0 8 】

相手先に本人だと認証されたら、相手先との取引が開始される。または、相手先が第3者である取引先に認証結果を送信し、使用者と第3者とが取引を開始しても良い。

【 0 0 0 9 】

上記本人認証作業において、使用者の生体情報が通信装置に記憶されている生体情報と合致しない場合、再び使用者の生体情報を通信装置に入力し直すことができる。通信装置に繰り返し生体情報を入力して照合を行おうとしたとき、連続してn回以上（nは自然数）合致しない場合は相手先に自動的にn回以上合致しなかったことを通知するようにしても良い。

【 0 0 1 0 】

また、通信装置に記憶されている使用者の生体情報は複数あっても良く、例えば、指紋と声紋の両方を通信装置に入力することで本人認証作業を行う構成にしても良い。そして通信装置に記憶されている使用者の生体情報を書き換える場合、一度通信装置を用いて本人認証作業を行った後、相手先に生体情報を書き換える際に必要な暗証番号を情報として送り、相手先において暗証番号が合致したら、通信装置に記憶されている生体情報を書き換えることができるようにしても良い。

【 0 0 1 1 】

また生体情報の通信装置への入力、CCDやフォトダイオードを用いたライセンサーやエリアセンサー、マイク等によって行われる。

【 0 0 1 2 】

上記構成によって、暗証番号が本人以外の人間に漏洩して使用者以外に悪用さ

れる可能性が低減する。そして、本人認証作業の際に、使用者と相手先との間においてデータをやりとりする必要がなくなるため、相手先との通信に必要なコストを抑えることができ、何らかのエラーにより通信が断絶し本人認証作業を最初から再び行うという繁雑さを回避することができる。さらに、使用者の生体情報を用いて認証を行うため、使用者が暗証番号を忘れて相手先に再び暗証番号を登録する必要がなくなる。また、暗証番号を通信機器に入力する手間を省くことができる。

【 0 0 1 3 】

以下に本発明の構成を示す。

【 0 0 1 4 】

本発明は、
顧客を識別する本人認証システムであって、
前記顧客の生体情報を記憶する手段と、
前記顧客の生体情報を読み取る手段と、
前記読み取った生体情報を前記記憶した生体情報と照合する手段と、
前記照合が合致した場合、サーバーに合致したことを情報として送る手段と、
を有することを特長とする。

【 0 0 1 5 】

本発明は、
顧客を識別する本人認証システムであって、
前記顧客の複数の生体情報を記憶する手段と、
前記顧客の生体情報を読み取る手段と、
前記読み取った生体情報を前記記憶した複数の生体情報と照合する手段と、
前記読み取った生体情報が、前記記憶した複数の生体情報のうち少なくとも1つと合致した場合、サーバーに合致したことを情報として送る手段と、
を有することを特長とする。

【 0 0 1 6 】

本発明は、
顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、
前記顧客の複数の生体情報を読み取る手段と、
前記読み取った複数の生体情報を前記記憶した複数の生体情報と照合する手段と、

前記読み取った複数の生体情報のそれぞれが、前記記憶した複数の生体情報のうち少なくとも1つと合致した場合、サーバーに合致したことを情報として送る手段と、

を有することを特長とする。

【 0 0 1 7 】

本発明は、
顧客を識別する本人認証システムであって、
前記顧客の生体情報を記憶する手段と、
前記顧客の生体情報を読み取る手段と、
前記読み取った生体情報を前記記憶した生体情報と照合する手段と、
前記照合が合致した場合、サーバーに合致したことを情報として、インターネットを介して送る手段と、
を有することを特長とする。

【 0 0 1 8 】

本発明は、
顧客を識別する本人認証システムであって、
前記顧客の複数の生体情報を記憶する手段と、
前記顧客の生体情報を読み取る手段と、
前記読み取った生体情報を前記記憶した複数の生体情報と照合する手段と、
前記照合の結果、前記読み取った生体情報が、前記記憶した複数の生体情報のうち少なくとも1つと合致した場合、サーバーに前記照合が合致したことを情報として、インターネットを介して送る手段と、
を有することを特長とする。

【 0 0 1 9 】

本発明は、

顧客を識別する本人認証システムであって、
前記顧客の複数の生体情報を記憶する手段と、
前記顧客の複数の生体情報を読み取る手段と、
前記読み取った複数の生体情報を前記記憶した複数の生体情報と照合する手段と、

前記照合の結果、前記読み取った複数の生体情報のそれぞれが、前記記憶した複数の生体情報のうち少なくとも1つと合致した場合、サーバーに前記照合が合致したことを情報として、インターネットを介して送る手段と、
を有することを特長とする。

【 0 0 2 0 】

本発明は、
顧客を識別する本人認証システムであって、
前記顧客の生体情報を記憶する手段と、
前記顧客の生体情報を読み取る手段と、
前記読み取った生体情報を前記記憶した生体情報と照合する手段と、
前記照合が合致した場合、サーバーに合致したことを情報として送る手段と、
前記サーバーが前記顧客の取引先に前記照合が合致したことを情報として送る手段と、
を有し、

前記取引先が、前記照合が合致したことを情報として受け取った後に、前記顧客と前記取引先との間で取引が開始されることを特長とする。

【 0 0 2 1 】

本発明は、
顧客を識別する本人認証システムであって、
前記顧客の複数の生体情報を記憶する手段と、
前記顧客の生体情報を読み取る手段と、
前記読み取った生体情報を前記記憶した複数の生体情報と照合する手段と、
前記照合の結果、前記読み取った生体情報が前記記憶した複数の生体情報のうち少なくとも1つと合致した場合、サーバーに前記照合が合致したことを情報と

して送る手段と、

前記サーバーが前記顧客の取引先に前記照合が合致したことを情報として送る手段と、

を有し、

前記取引先が、前記照合が合致したことを情報として受け取った後に、前記顧客と前記取引先との間で取引が開始されることを特長とする。

【 0 0 2 2 】

本発明は、

顧客を識別する本人認証システムであって、

前記顧客の複数の生体情報を記憶する手段と、

前記顧客の複数の生体情報を読み取る手段と、

前記読み取った複数の生体情報を前記記憶した複数の生体情報と照合する手段と、

前記照合の結果、前記読み取った複数の生体情報のそれぞれが、前記記憶した複数の生体情報のうち少なくとも1つと合致した場合、サーバーに前記照合が合致したことを情報として送る手段と、

前記サーバーが前記顧客の取引先に前記照合が合致したことを情報として送る手段と、

を有し、

前記取引先が、前記照合が合致したことを情報として受け取った後に、前記顧客と前記取引先との間で取引が開始されることを特長とする。

【 0 0 2 3 】

本発明は、

顧客を識別する本人認証システムであって、

前記顧客の生体情報を記憶する手段と、

前記顧客の生体情報を読み取る手段と、

前記読み取った生体情報を前記記憶した生体情報と照合する手段と、

前記照合が合致した場合、サーバーに合致したことを情報として送る手段と、
を有し、

前記サーバーに前記照合が合致したことを情報として送った後に、暗証番号を情報として前記サーバーに送り、前記サーバーにおいて記憶されている番号と前記暗証番号が合致した場合、前記記憶された生体情報を書き換えられることを特長とする。

【 0 0 2 4 】

本発明は、
顧客を識別する本人認証システムであって、
前記顧客の複数の生体情報を記憶する手段と、
前記顧客の生体情報を読み取る手段と、
前記読み取った生体情報を前記記憶した複数の生体情報と照合する手段と、
前記読み取った生体情報が、前記記憶した複数の生体情報のうち少なくとも1つと合致した場合、サーバーに合致したことを情報として送る手段と、
を有し、

前記サーバーに前記照合が合致したことを情報として送った後に、暗証番号を情報として前記サーバーに送り、前記サーバーにおいて記憶されている番号と前記暗証番号が合致した場合、前記記憶された複数の生体情報を書き換えられることを特長とする。

【 0 0 2 5 】

本発明は、
顧客を識別する本人認証システムであって、
前記顧客の複数の生体情報を記憶する手段と、
前記顧客の複数の生体情報を読み取る手段と、
前記読み取った複数の生体情報を前記記憶した複数の生体情報と照合する手段と、
前記読み取った複数の生体情報のそれぞれが、前記記憶した複数の生体情報のうち少なくとも1つと合致した場合、サーバーに合致したことを情報として送る手段と、
を有し、

前記サーバーに前記照合が合致したことを情報として送った後に、暗証番号を

情報として前記サーバーに送り、前記サーバーにおいて記憶されている番号と前記暗証番号が合致した場合、前記記憶された複数の生体情報を書き換えられることを特長とする。

【 0 0 2 6 】

本発明は、前記顧客と前記取引先との間で行われる取引が前記サーバーに設定された条件を満たす場合のみ、前記顧客の識別を要求することを特長としていても良い。

【 0 0 2 7 】

前記生体情報とは、指紋、掌紋または声紋であることを特長としていても良い。

【 0 0 2 8 】

前記掌紋は手ひらの全体の掌紋、もしくは前記手のひらの一部の掌紋であることを特徴としていても良い。

【 0 0 2 9 】

前記顧客の生体情報を記憶する手段とは、フラッシュメモリであることを特長としていても良い。

【 0 0 3 0 】

前記顧客の生体情報を読み取る手段とは、フォトダイオードまたはCCDであることを特長としていても良い。

【 0 0 3 1 】

本発明は、携帯情報端末、携帯電話またはパーソナルコンピュータを用いることを特長としていても良い。

【 0 0 3 2 】

【発明の実施の形態】

図1に本発明の本人認証システムのフローを示す。まず通信装置の操作キーを操作し、生体情報を収集する。あらかじめプログラムされていれば、1つの操作キーを押すことによって生体情報の収集が開始されるようにすることも可能である。また、通信装置の電源投入時に自動的に生体情報収集がはじめられるようにすることも可能である。

【 0 0 3 3 】

得られた生体情報は、あらかじめ通信装置の中の不揮発性メモリなどで形成されている内蔵メモリに蓄えられている本人の生体情報（内蔵メモリデータ）と比較される。ここで、2つの生体情報が合致すると判断されれば、使用者は通信装置の正しい所有者であると認証される。認証終了後、認証済であるという情報を有するデータを相手先に送信する。このとき、認証作業はすでに終了しているので、新たに相手先との間で認証作業をする必要はなく、通信装置から認証は終了しているという情報を相手先は受け取るだけでよい。

【 0 0 3 4 】

本実施の形態の本人認証システムに使用する通信装置はセンサーまたはマイクを内蔵している。ここで用いるセンサーはラインセンサーまたはエリアセンサーであり、使用者の生体情報を読み取るのに使用する。

【 0 0 3 5 】

次に、本発明の本人認証システムに用いられる生体情報のうち、指紋及び掌紋について説明する。

【 0 0 3 6 】

図2に人間の右手を示す。生体情報として通信装置に読み取られるのは、手のひらの一部である掌紋1、手のひら全体である掌紋2、親指の指紋、人差し指の指紋、中指の指紋、薬指の指紋または小指の指紋である。上記生体情報のうち、1つの生体情報だけを通信機器に記憶させても良いし、複数の生体情報を記憶させても良い。

【 0 0 3 7 】

手のひらの一部である掌紋1、手のひら全体である掌紋2、親指の指紋、人差し指の指紋、中指の指紋、薬指の指紋及び小指の指紋は、個々の人間に特有のものであるため、第3者による通信装置の悪用を防ぐことができる。

【 0 0 3 8 】

本人認証作業が終了し、相手先が認証終了の情報を通信装置から受け取ると、使用者と相手先との間で取引が開始される。または、相手先が第3者である取引先に認証結果を送信し、使用者と第3者である取引先とが取引を開始しても良い。

【 0 0 3 9 】

図 3 に使用者と第 3 者である取引先とが取引する場合のフローを示す。まず使用者が通信装置を用いて本人認証作業を終了したら、通信装置から相手先（サーバー）に本人認証作業が終了したという情報が送信される。

【 0 0 4 0 】

サーバーは、本人認証作業が終了したという情報を受け取ったら、第 3 者としての取引先に、本人認証済であるという情報を送信する。本人認証済であるという情報を受け取った取引先は、直接使用者と取引を開始する。

【 0 0 4 1 】

上記構成によって、暗証番号が本人以外の人間に漏洩して使用者以外に悪用される可能性が低減する。そして、本人認証作業の際に、使用者と相手先との間においてデータをやりとりする必要がなくなるため、相手先との通信に必要なコストを抑えることができ、何らかのエラーにより通信が断絶し本人認証作業を最初から再び行うという繁雑さを回避することができる。さらに、使用者の生体情報を用いて認証を行うため、使用者が暗証番号を忘れて相手先に再び暗証番号を登録する必要がなくなる。また、暗証番号を通信機器に入力する手間を省くことができる。

【 0 0 4 2 】

【実施例】

以下に、本発明の実施例について説明する。

【 0 0 4 3 】

（実施例 1）

以下に本発明において用いられる通信装置の構成と、その動作について説明する。

【 0 0 4 4 】

図 4 は本実施例の通信装置のブロック図である。この通信装置はアンテナ 6 0 1、送信受信回路 6 0 2、信号を圧縮伸張化、符号化する信号処理回路 6 0 3、制御用マイコン 6 0 4、フラッシュメモリ 6 0 5、操作キー 6 0 6などを有して

いる。そしてさらに、センサー 6 1 1、照合回路部 6 1 2などを有している。

【 0 0 4 5 】

操作キー 6 0 6を操作することによって、制御用マイコン 6 0 4がセンサー 6 1 1を制御し、使用者の生体情報を読み取らせる。なお本実施例では、生体情報として、掌紋または指紋を用いる例について説明する。センサー 6 1 1で読み取った使用者の生体情報は、照合回路部 6 1 2に入力される。

【 0 0 4 6 】

照合回路部 6 1 2に入力された使用者の生体情報は、A/Dコンバータ 6 1 3においてデジタル信号に変換される。デジタル信号に変換された使用者の生体情報は、DSP（デジタルシグナルプロセッサ）6 1 4に入力され、信号処理される。信号処理とは具体的には、生体情報をより判別しやすくするため、微分フィルタなどを用い映像の濃淡が変わるところを際立たせることである。得られた生体情報はDSP 6 1 4内部で数値化され、比較回路 6 1 5に入力される。

【 0 0 4 7 】

比較回路 6 1 5はフラッシュメモリ 6 0 5に記憶されている基準となる使用者の生体情報と、DSP 6 1 4内部で数値化され比較回路 6 1 5に入力された生体情報とを比較照合する。

【 0 0 4 8 】

生体情報を照合する方法としては、基準となる生体情報と収集した生体情報のそれぞれの特徴を比較して照合する特徴照合方式と、該二つの生体情報を直接比較する画像マッチング方式があるが、どちらの方式を用いても良い。また基準データは1つだけではなく、手の向きを多少変えるなどして、複数の認証データを備えたほうがより確実な認証が可能となる。

【 0 0 4 9 】

ここで合致が見られれば、制御用マイコン 6 0 4は認証信号を出力し、該認証信号は、信号処理回路 6 0 3、送受信回路 6 0 2、アンテナ 6 0 1を介して通信装置から出力される。通信装置から出力された認証信号は、インターネットなどを通じて伝達される。なお、通信装置から出力された認証信号を、インターネットを介さず直接相手先に送信しても良い。

【 0 0 5 0 】

(実施例 2)

以下に本発明において用いられる通信装置の構成と、その動作の、実施例 1 とは異なる例について説明する。

【 0 0 5 1 】

図 5 は本実施例の通信装置のブロック図である。この通信装置はアンテナ 5 0 1、送信受信回路 5 0 2、信号を圧縮伸張化、符号化する信号処理回路 5 0 3、制御用マイコン 5 0 4、フラッシュメモリ 5 0 5、操作キー 5 0 6などを有している。そしてさらに、マイク 5 1 1、アンプ 5 1 6、照合回路部 5 1 2などを有している。

【 0 0 5 2 】

操作キー 5 0 6を操作することによって、制御用マイコン 5 0 4がマイク 5 1 1を制御し、使用者の生体情報を読み取らせる。なお本実施例では、生体情報として、声紋を用いる例について説明する。マイク 5 1 1で読み取った使用者の生体情報は、アンプ 5 1 6によって増幅され、照合回路部 5 1 2に入力される。

【 0 0 5 3 】

照合回路部 5 1 2に入力された使用者の生体情報は、A/Dコンバータ 5 1 3においてデジタル信号に変換される。デジタル信号に変換された使用者の生体情報は、DSP (デジタルシグナルプロセッサ) 5 1 4に入力され、信号処理される。信号処理とは具体的には、生体情報をより判別しやすくするため、帯域フィルタなどを用い、周波数ごとの音の強さを数値化することである。DSP 5 1 4により数値化された生体情報は比較回路 5 1 5に入力される。

【 0 0 5 4 】

比較回路 5 1 5はフラッシュメモリ 5 0 5に記憶されている基準となる使用者の生体情報と、DSP 5 1 4内部で数値化され比較回路 5 1 5に入力された生体情報とを比較照合する。

【 0 0 5 5 】

生体情報を照合する方法としては、基準となる生体情報と収集した生体情報のそれぞれの特徴を比較して照合する特徴照合方式と、該二つの生体情報が有する

スペクトルを直接比較する画像マッチング方式があるが、どちらの方式を用いても良い。また基準データは1つだけではなく、発音を多少変えるなどして、複数の認証データを備えたほうがより確実な認証が可能となる。

【0056】

ここで合致が見られれば、制御用マイコン504は認証信号を出力し、該認証信号は、信号処理回路503、送受信回路502、アンテナ501を介して通信装置から出力される。通信装置から出力された認証信号は、インターネットなどを通じて伝達される。なお、通信装置から出力された認証信号を、インターネットを介さず直接相手先に送信しても良い。

【0057】

本実施例の構成は、実施例1と自由に組み合わせて実施することが可能である。

【0058】

(実施例3)

次に本発明で用いられる通信装置の1つである、携帯情報端末について述べる。図6に示すのは本実施例の携帯情報端末であり、2701は表示用パネル、2702は操作用パネルである。表示用パネル2701と操作用パネル2702は接続部2703において接続されている。そして接続部2703における、表示用パネル2701のセンサー内蔵ディスプレイ2704が設けられている面と操作用パネル2702の音声入力部2708が設けられている面との角度 θ は、任意に変えることができる。

【0059】

表示用パネル2701はセンサー内蔵ディスプレイ2704を有している。センサー内蔵ディスプレイ2704はセンサーとしての機能する他に、ディスプレイとしても機能し、画像を表示することが可能である。本実施例ではセンサー内蔵ディスプレイ2704にはELディスプレイが用いられている。

【0060】

また図6に示した携帯情報端末は電話としての機能を有しており、表示用パネル2701は音声出力部2705を有しており、音声は音声出力部2705から

出力される。

【0061】

操作用パネル2702は操作キー2706、電源スイッチ2707、音声入力部2708を有している。なお図6では操作キー2706と電源スイッチ2707とを別個に設けたが、操作キー2706の中に電源スイッチ2707が含まれる構成にしても良い。音声入力部2708において、音声が入力される。

【0062】

なお図6では表示用パネル2701が音声出力部2705を有し、操作用パネル2702が音声入力部2708を有しているが、本実施例はこの構成に限定されない。表示用パネル2701が音声入力部2708を有し、操作用パネルが音声出力部2705を有していても良い。また音声出力部2705と音声入力部2708とが共に表示用パネル2701に設けられていても良いし、音声出力部2705と音声入力部2708とが共に操作用パネル2702に設けられていても良い。

【0063】

図7、図8を用いて、図6で示した携帯情報端末の使用方法について説明する。図7に示すように、図6で示した携帯情報端末によって認証を行う場合には、手のひらをセンサー内蔵ディスプレイ2704に覆いかぶせるようにして使用する。認証は操作キー2706でキー操作を行うとともに、使用者の手相をセンサー内蔵ディスプレイ2704が読み取り、認証作業を行う。

【0064】

なお図7では操作キー2706を人差し指で操作している例について示したが、図8に示すように、親指で操作キー2706を操作することも可能である。なお操作キー2706は操作用パネル2702の側面に設けても良い。操作は片手（きき手）の人差し指のみ、または親指のみでも可能である。

【0065】

以下に図6に示した携帯情報端末の構成と、その動作について説明する。

【0066】

図9は本実施例の携帯情報端末のブロック図である。この携帯情報端末はアン

テナ 9 0 1、送信受信回路 9 0 2、信号を圧縮伸張化、符号化する信号処理回路 9 0 3、制御用マイコン 9 0 4、フラッシュメモリ 9 0 5、操作キー 9 0 6、音声入力回路 9 0 7、音声出力回路 9 0 8、マイク 9 0 9、スピーカ 9 1 0などを有している。そしてさらに、センサー 9 1 1、照合回路部 9 1 2などを有している。

【 0 0 6 7 】

音声入力部 2 7 0 8 から入力された音声は、マイク 9 0 9 に入力され、アナログ信号として音声入力回路 9 0 7 に入力される。音声入力回路 9 0 7 に入力されたアナログ信号は増幅された後デジタル信号に変換され、信号処理部 9 0 3 に入力される。信号処理部 9 0 3 において圧縮伸張化、符号化されたデジタル信号は、送受信回路 9 0 2 において周波数を変えられて、場合によっては増幅されて、アンテナ 9 0 1 から送信される。

【 0 0 6 8 】

またアンテナ 9 0 1 において受信した音声情報を有するデジタル信号は、送受信回路 9 0 2 において周波数を変えられて、場合によっては増幅されて、信号処理部 9 0 3 に入力される。信号処理部 9 0 3 に入力されたデジタル信号は圧縮伸張化、符号化され、音声出力回路 9 0 8 に入力される。音声出力回路 9 0 8 に入力されたデジタル信号はアナログ信号に変換された後増幅され、スピーカ 9 1 0 から出力され、音声出力部 2 7 0 8 から音声として使用者の耳に入力する。

【 0 0 6 9 】

操作キー 9 0 6 を操作することによって、制御用マイコン 9 0 4 がセンサー 9 1 1 を制御し、使用者の生体情報を読み取らせる。なお本実施例では、生体情報として、掌紋または指紋を用いる例について説明する。センサー 9 1 1 で読み取った使用者の生体情報は、照合回路部 9 1 2 に入力される。

【 0 0 7 0 】

照合回路部 9 1 2 に入力された使用者の生体情報は、A/Dコンバータ 9 1 3 においてデジタル信号に変換される。デジタル信号に変換された使用者の生体情報は、DSP（デジタルシグナルプロセッサ）9 1 4 に入力され、信号処理される。信号処理とは具体的には、生体情報をより判別しやすくするため、微分フイ

ルタなどを用い映像の濃淡が変わるところを際立たせることである。得られた生体情報はDSP914内部で数値化され、比較回路915に入力される。

【0071】

比較回路915はフラッシュメモリ905に記憶されている基準となる使用者の生体情報と、DSP914内部で数値化され比較回路915に入力された生体情報とを比較照合する。

【0072】

生体情報を照合する方法としては、基準となる生体情報と収集した生体情報のそれぞれの特徴を比較して照合する特徴照合方式と、該二つの生体情報を直接比較する画像マッチング方式があるが、どちらの方式を用いても良い。また基準データは1つだけではなく、手の向きを多少変えるなどして、複数の認証データを備えたほうがより確実な認証が可能となる。

【0073】

ここで合致が見られれば、制御用マイコン904は認証信号を出力し、該認証信号は、信号処理回路903、送受信回路902、アンテナ901を介して携帯情報端末から出力される。携帯情報端末から出力された認証信号は、インターネットなどを通じて伝達される。なお、携帯情報端末から出力された認証信号を、インターネットを介さず直接相手先に送信しても良い。

【0074】

なお本発明で用いられる通信装置は、本実施例で示した構成の携帯情報端末に限定されない。また本実施例で示した携帯情報端末は、指紋または掌紋を生体情報として利用しているが、声紋を生体情報として利用する構成を有していても良い。

【0075】

なお、本実施例は、実施例1または2と自由に組み合わせて実施することが可能である。

【0076】

(実施例4)

本実施例は本発明を使用する状況を述べるものである。本人認証が生体情報ま

での高度な認証が不要な場合は本発明を使用しないこともありえる。小額の金銭移動などの場合は必ずしも必要ではない。

【 0 0 7 7 】

このため、認証の有無が選択できること、たとえば金銭が高額な移動が伴う場合のみに選択的に認証が出来るようにすることも可能である。取引先の状況に合わせて使用することや、あらかじめ携帯情報装置の制御マイコン上に判定基準を設定しておき、数値が一定値を超えた場合のみ使用することが可能である。また、認証結果を必要な場合のみ認証結果をインターネットで伝達することも可能である。

【 0 0 7 8 】

なお、本実施例は、実施例 1 ～ 実施例 3 と自由に組み合わせて実施することが可能である。

【 0 0 7 9 】

(実施例 5)

本発明に用いられる通信装置として、様々な電子機器を用いることができる。

【 0 0 8 0 】

図 1 0 (A) はパーソナルコンピューター (パソコン) であり、本体 2 5 0 1 、筐体 2 5 0 2 、表示部 2 5 0 3 、キーボード 2 5 0 4 、センサー 2 5 0 5 等を含む。本発明では、センサー 2 5 0 5 を用い、パーソナルコンピューター内に生体情報を取り込むことができる。

【 0 0 8 1 】

なお本実施例では、指紋または掌紋を生体情報として利用する例について示したが、音声入力部を設けて声紋を生体情報として利用する構成にしても良い。またセンサー 2 5 0 5 と音声入力部を両方設けて、指紋または掌紋と、声紋とを共に利用する構成にしても良い。

【 0 0 8 2 】

図 1 0 (B) は携帯電話であり、本体 2 6 0 1 、音声出力部 2 6 0 2 、音声入力部 2 6 0 3 、表示部 2 6 0 4 、操作キー 2 6 0 5 、アンテナ 2 6 0 6 を含んでいる。通常の電話をかける場合は表示部 2 6 0 4 に相手先の電話番号や、電波の

受信状態などが表示される。また、インターネットを使用する場合には、相手先の必要情報が表示されることになる。そして表示部 2 6 0 4 はセンサーとしても機能し、表示部 2 6 0 4 において生体情報を取り込むことが可能である。

【0 0 8 3】

また、図 1 0 (B) に示した携帯電話は、表示部 2 6 0 4 がセンサーとしての機能とディスプレイとしての機能を併せ持っていたが、表示部 2 6 0 4 をディスプレイとしてのみ利用し、センサーを別個に設ける構成にしても良い。

【0 0 8 4】

なお本発明で用いられる通信装置は本実施例で示した電子機器に限定されない。生体情報を取り込み、該生体情報をあらかじめ記憶されている生体情報と照合し、照合が合致したら相手先に認証が終了したことを知らせる機能を有していればよい。

【0 0 8 5】

【発明の効果】

本発明の本人認証システムは、暗証番号が本人以外の人間に漏洩して使用者以外に悪用される可能性が低減する。そして、本人認証作業の際に、使用者と相手先との間においてデータをやりとりする必要がなくなるため、相手先との通信に必要なコストを抑えることができ、何らかのエラーにより通信が断絶し本人認証作業を最初から再び行うという繁雑さを回避することができる。さらに、使用者の生体情報を用いて認証を行うため、使用者が暗証番号を忘れて相手先に再び暗証番号を登録する必要がなくなる。また、暗証番号を通信機器に入力する手間を省くことができる。

【図面の簡単な説明】

【図 1】 本発明の本人認証システムのフロー。

【図 2】 読み取る掌紋または指紋の位置を示す図。

【図 3】 使用者とサーバーと第 3 者としての取引先の関係を示した図。

【図 4】 通信装置の構造を示すブロック図。

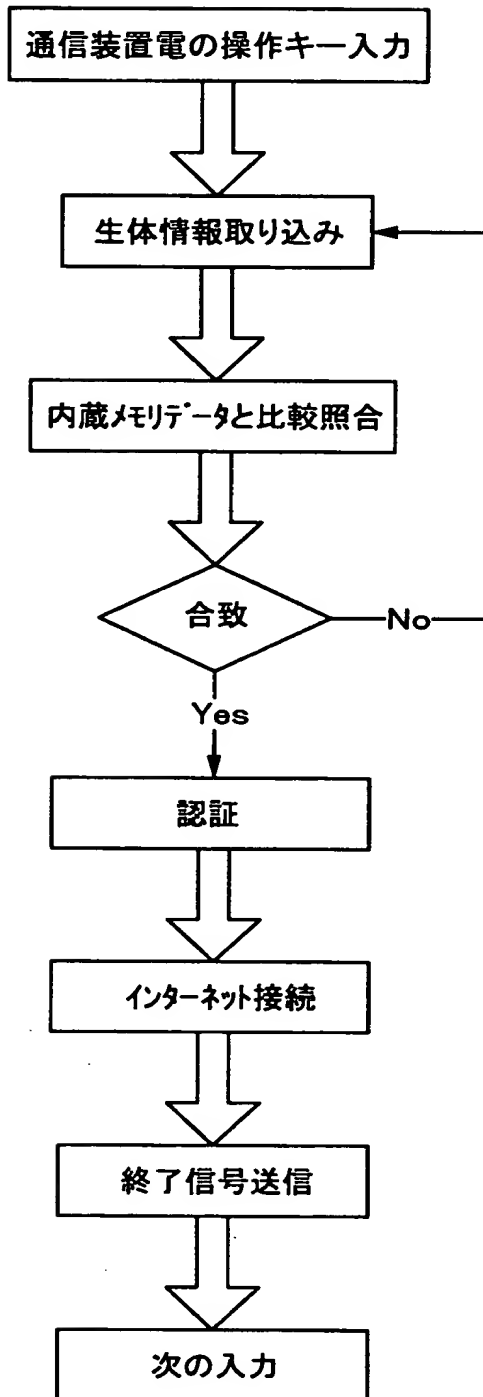
【図 5】 通信装置の構造を示すブロック図。

【図 6】 通信装置の一例である携帯情報端末の外観図。

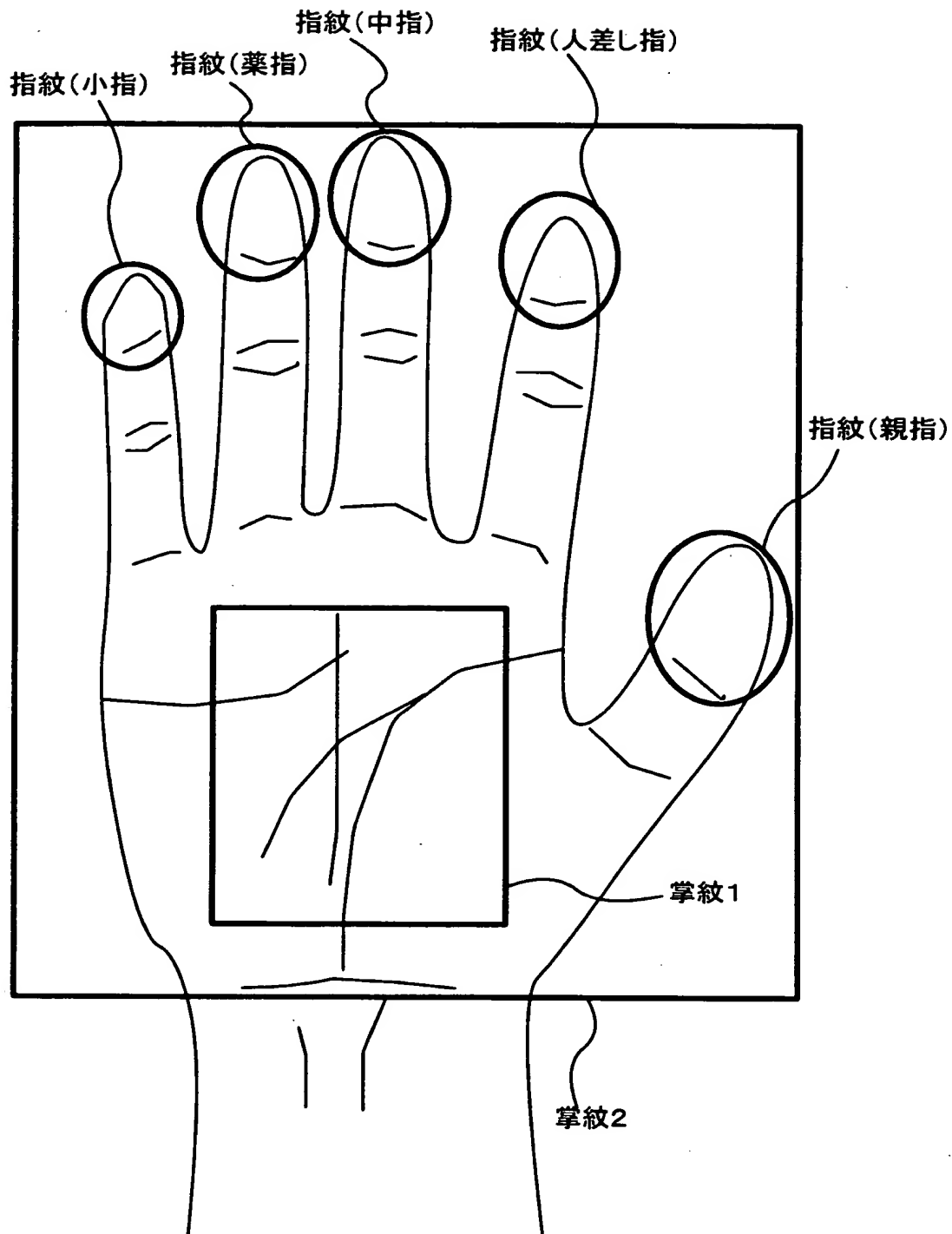
- 【図 7】 通信装置の一例である携帯情報端末の使用例。
- 【図 8】 通信装置の一例である携帯情報端末の使用例。
- 【図 9】 通信装置の一例である携帯情報端末の構造を示すブロック図。
- 【図 1 0】 通信装置の一例である電子機器の図。
- 【図 1 1】 従来の本人認証のフロー。

【書類名】 図面

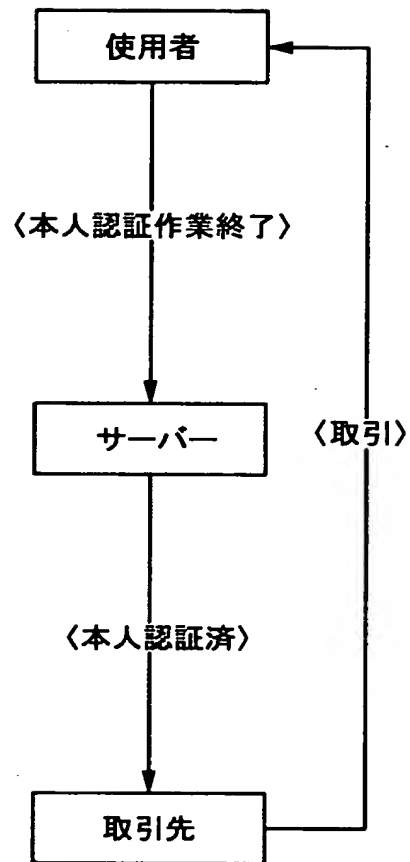
【図 1】



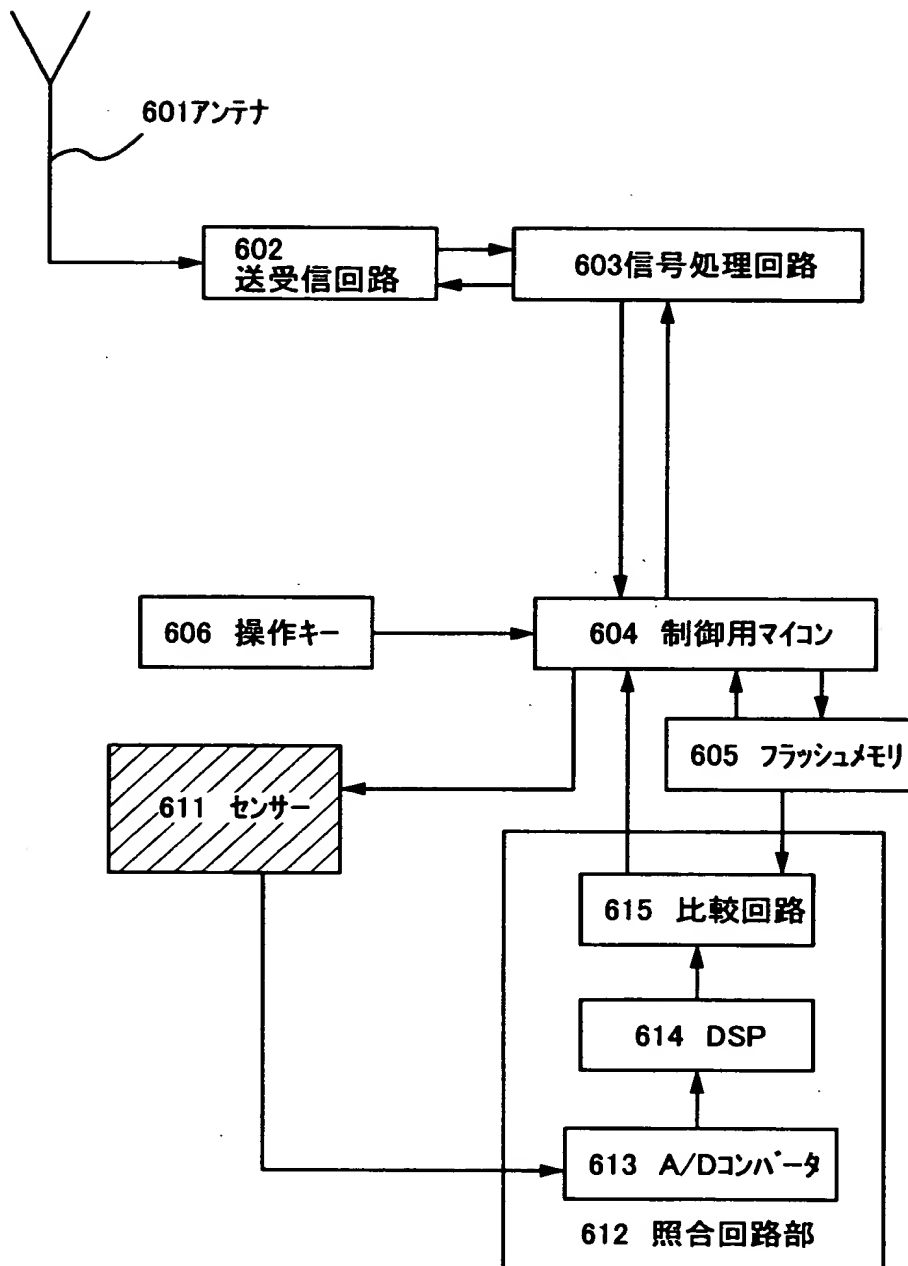
【図2】



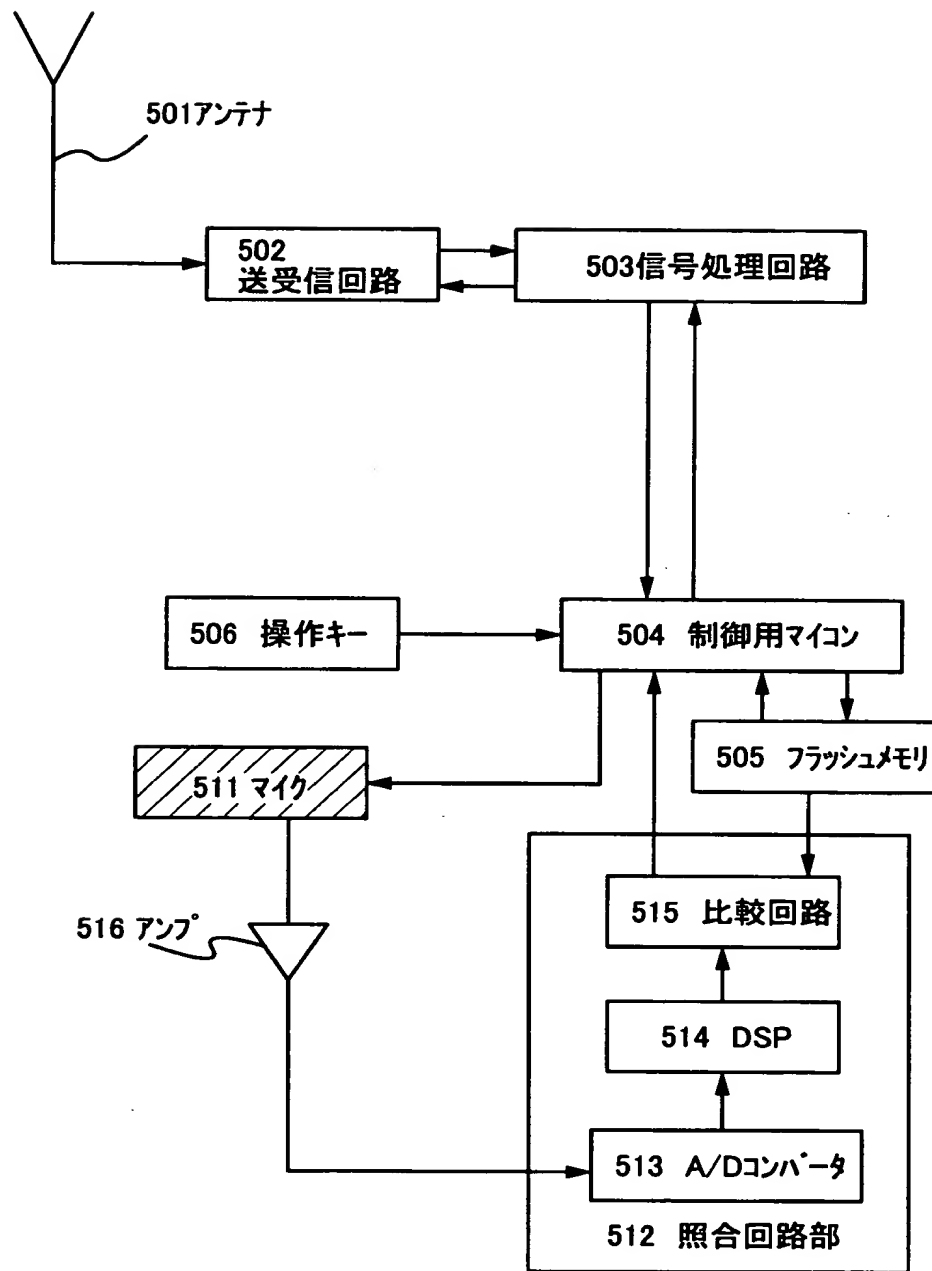
【図 3】



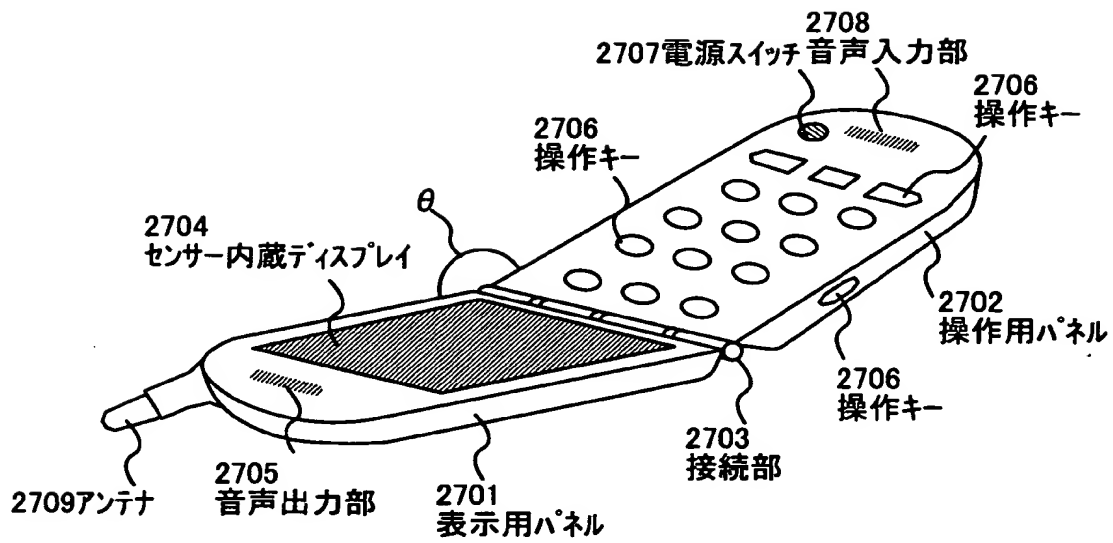
【図4】



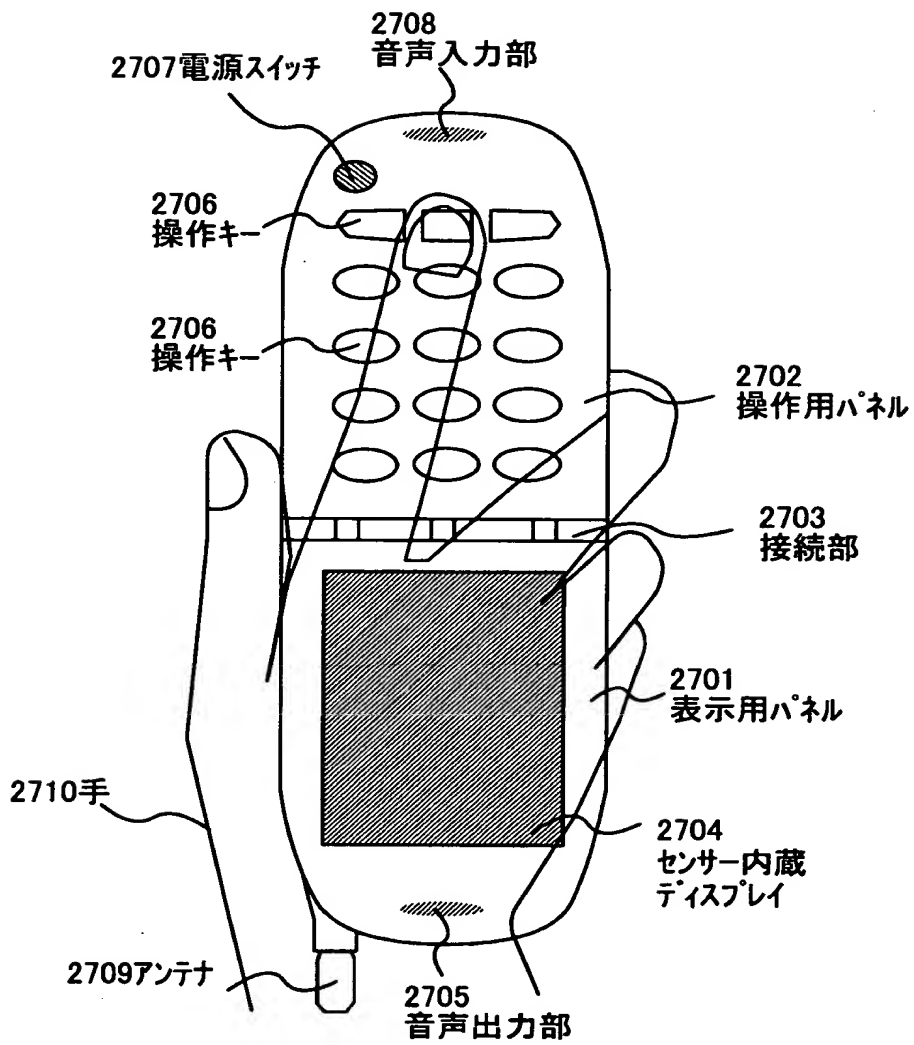
【図 5】



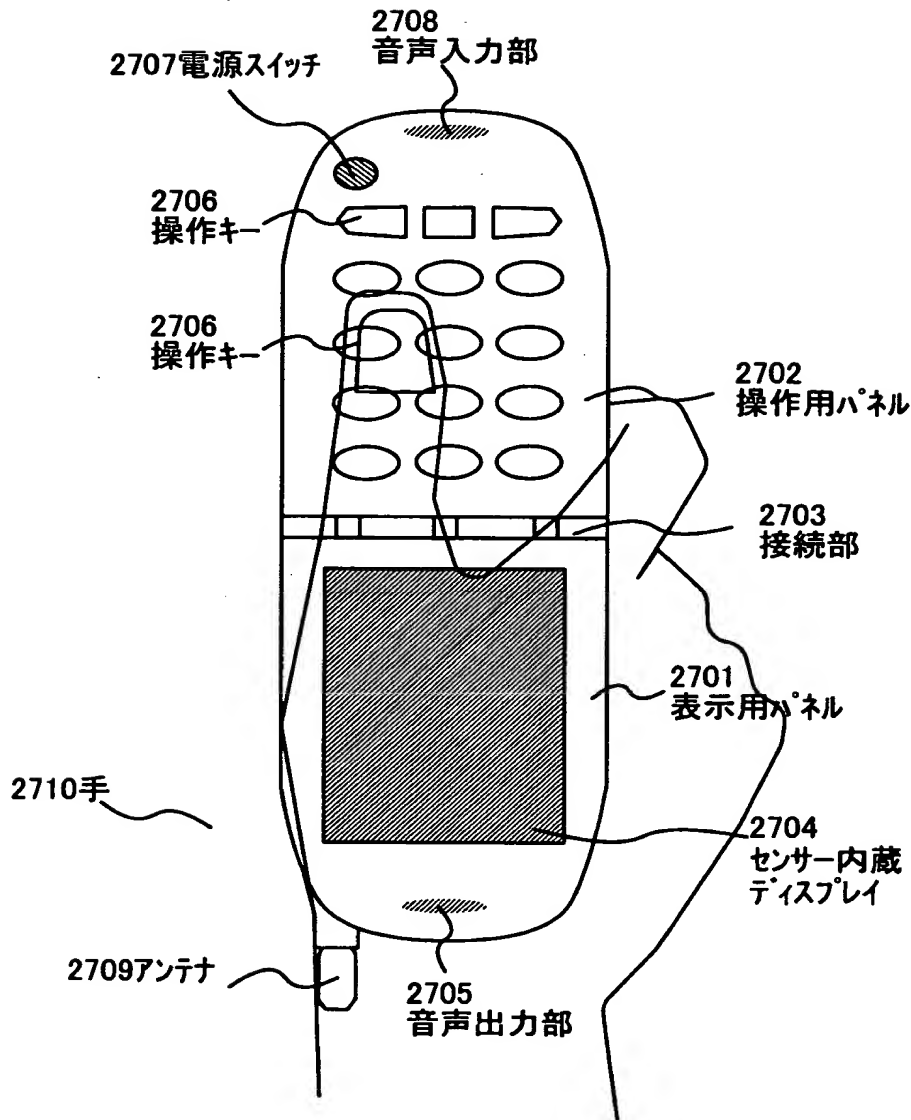
【図 6】



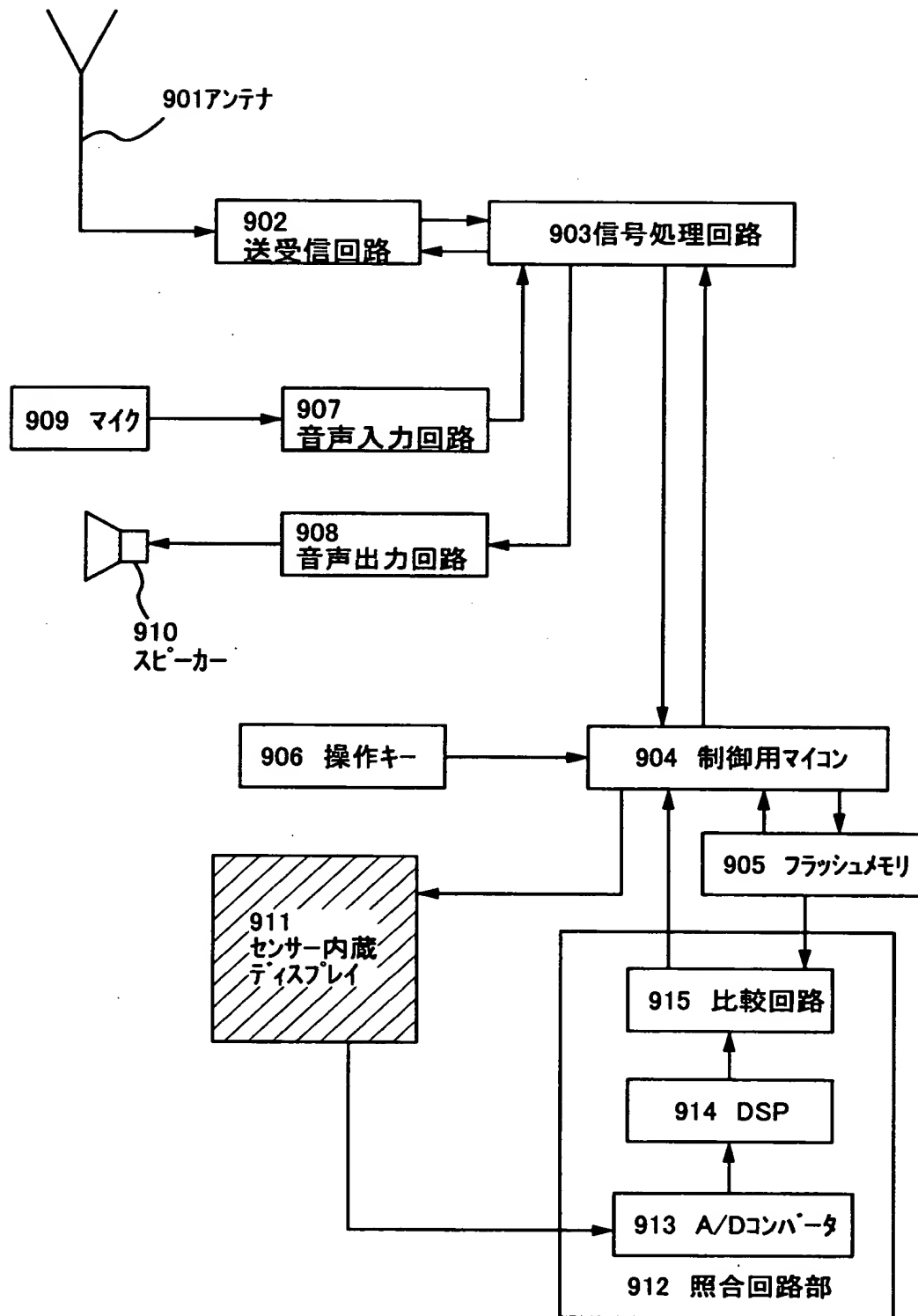
【図 7】



【図 8】

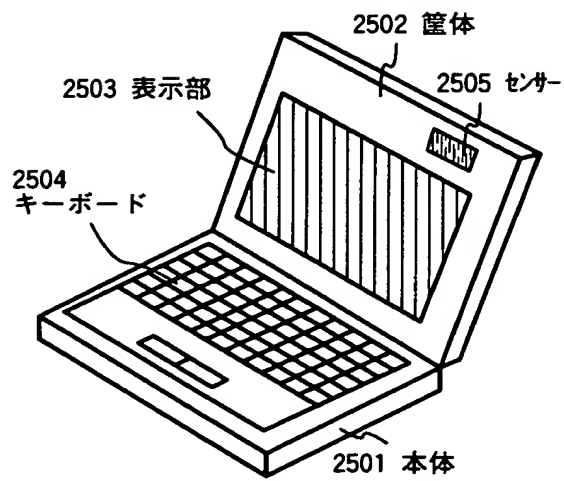


【図 9】

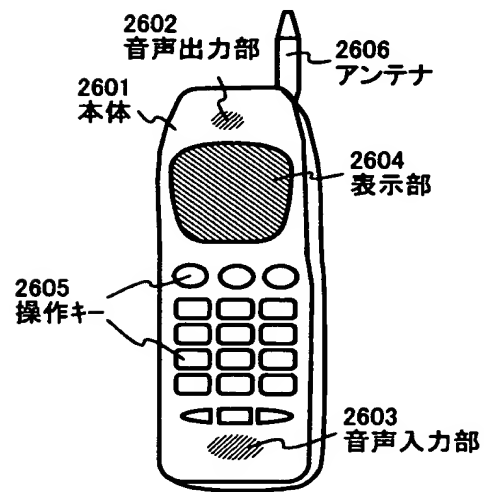


【図 1 0】

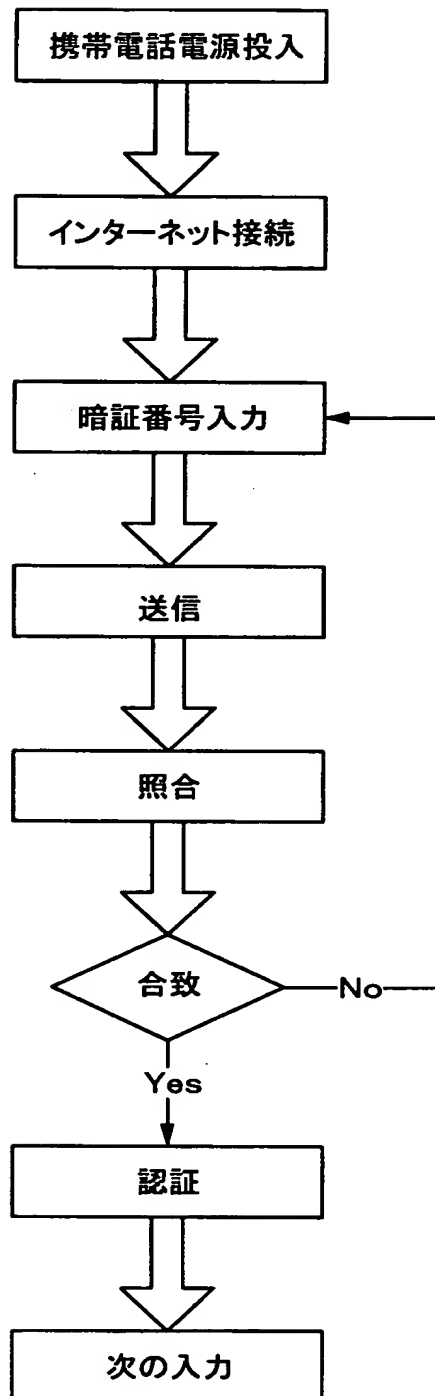
(A)



(B)



【図 1 1】



【書類名】 要約書

【要約】

【課題】 顧客識別が容易な本人認証システムを提供する。

【解決手段】 顧客を識別する本人認証システムであって、前記顧客の生体情報を記憶する手段と、前記顧客の生体情報を読み取る手段と、前記読み取った生体情報を前記記憶した生体情報と照合する手段と、前記照合が合致した場合、サーバーに合致したことを情報として送る手段とを有することを特長とする本人認証システム。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000153878]

1. 変更年月日 1990年 8月17日

[変更理由] 新規登録

住 所 神奈川県厚木市長谷398番地

氏 名 株式会社半導体エネルギー研究所